PREVENTING EMPLOYEE THEFT
SDPD Neighborhood Policing Resource Team
April 29, 2016

CONTENTS

PERSONNEL POLICIES
CASH HANDLING
COMPUTER SECURITY
DOCUMENT PROTECTION
INVENTORY CONTROL
TRASH CONTROL
PURCHASING AND ACCOUNTING PROCEDURES
BANK DEPOSITS
KEY CONTROL
ACCESS CONTROL CARDS
SHIPPING AND RECEIVING PROCEDURES
PROPERTY IDENTIFICATION
SELECTING CONTRACTORS
TECHNOLOGY SOLUTIONS

According to the 2015 National Retail Security Survey Final Report, retailers in the United States lost about $15 billion to employee theft in 2014. This is about 34 percent of all retail theft losses, which totaled about $44 billion. Other sources of retail losses are shoplifting and organized retail crime (38 percent), administrative and paperwork error (16 percent), vendor fraud (7 percent), and other (5 percent). The U.S. Department of Commerce has estimated that more than 30 percent of all business failures are directly related to employee theft or fraud.

Nearly all businesses experience some employee theft. Most of it is undetected. It's estimated that less than 10 percent of a businesses' employees are responsible for more that 95 percent of the losses. One way of controlling employee theft is to develop a good relationship with your employees. Make them feel respected and reward them for doing their jobs well. Make sure they never feel wronged or slighted and might want to "get back" at your business. Provide good career opportunities. Businesses with the lowest turnover rates have been found to have the lowest employee theft rates. Other ways to prevent employee theft are outlined in this paper. They deal with personnel policies, cash handling, computer security, document protection, inventory control, mail room security, trash control, purchasing and accounting procedures, bank deposits, key control, access control cards, shipping and receiving procedures, property identification, selecting contractors, and technology solutions. After implementing these theft-prevention measures look to see if there are still ways for someone to steal from the business or otherwise harm it. Take additional measures if necessary.

Despite your best efforts, dishonest employees can usually find ways to steal. If you suspect theft, call your security or loss prevention manager and then the SDPD at **(619) 531-2000** or **(858) 484-3154**. Don't play detective and try to solve the crime. And don't jump to unwarranted conclusions. Be extremely careful about making accusations and conducting investigations. A false accusation could result in serious civil liability. Verify suspicions by careful investigations. If you can identify the responsible employee, terminate his or her employment and then consider further legal action. There should be no tolerance of employee theft or fraud, no matter how small. If the extent of the theft is large and complex, consider involving legal counsel who can assist in finding experts such as forensic accountants.

PERSONNEL POLICIES

In addition to theft, employees can do a great deal of damage to a business by ignorance of security policies, negligence in protecting business secrets, deliberate acts of sabotage, embezzlement, and the public release of sensitive information. The following measures will help prevent this.

- The first step in controlling employee theft is effective pre-employment screening. Conduct a comprehensive background check on prospective employees. Check references, credit reports, schools attended, licenses, civil judgments, citizenship, criminal records, and personality traits. Unless your business has sufficient in-house expertise and resources for this, you should contract with a knowledgeable and reputable Consumer Reporting Agency (CRA) that is familiar with and will comply with the federal Fair Credit Reporting Act (FCRA), California Investigative Consumer Reporting Agencies Act (UCRAA), Consumer Credit Reporting Agencies Act (CCRAA), and other laws enacted to protect consumers and job applicants. Here a consumer report is defined as any report by a third-party agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. For checks on foreigners, look for a CRA with a presence in the candidate's country of citizenship. And test the CRA by giving it an "applicant" whose background is known so it's the thoroughness and accuracy of its report can be assessed. You should also consult with legal counsel to ensure compliance with federal, state, and local laws. And with so many foreigners being employed, it is also necessary to comply with the laws governing a candidate's country of citizenship. Background checks are heavily regulated and even unintentional mistakes can lead to liability exposure. Care must be taken to achieve compliance with all relevant laws any time an employer starts to investigate the background of a job applicant. Here are some tips to avoid legal liability.
  - Don't randomly require background checks. Inconsistency in their use invites claims of discrimination.
  - Get the applicant's written consent for the background check in a stand-alone document that clearly states the intent of each report.
  - Make sure you use the correct forms.
  - Don't assume you can search public records and avoid liability.
  - Obtain reports from trusted sources. Extra care should be exercised when gathering information from unknown or unverifiable online repositories.
  - Don't ask applicants to self-identify criminal history. More and more jurisdictions are banning early requests for criminal background. In some jurisdictions, including a number of larger cities, employers cannot even ask about arrest history except in limited circumstances. The requirements also vary by type of employer.
  - Don't seek protected data, such as medical data, genetic information, or family status. If it is impermissible to ask for such information in an interview, it is likely impermissible for a CRA to obtain.
  - Don't seek data that is too old. Consumer reports should not extend past the last 10 years. Any other information more than seven years old except criminal convictions is also usually off limits.
  - Keep all background check reports and other documents. There are special rules for disposing of a consumer report.
  - Review each report carefully to determine if there's a job-related basis to disqualify an applicant.
  - Don't rush through the process or cut corners.
- A criminal record check should include arrests, convictions, and outstanding warrants. In considering this information in making employment decisions, follow the U.S. Equal Employment Opportunity Commission (EEOC) Enforcement Guidance No. 915.002 dated 4/25/2012 regarding the prohibition of discrimination under Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e *et seq*. Best practices for employers include the following:
  - Eliminate policies or practices that exclude people from employment based on any criminal record.
  - Train managers and hiring officials in the EEOC Enforcement Guidance.
  - Develop a policy and narrowly-tailored procedures for screening applicants and employees for criminal conduct.
  - Identify essential job requirements and the actual circumstances under which the jobs are performed.
  - Determine the specific offenses that may demonstrate unfitness for performing such jobs.
  - Identify the criminal offenses based on all available evidence.
  - Determine the duration of exclusions for criminal conduct based on all available evidence.
  - Include procedures for individualized assessments.

- Check the applicant's references. This can be very useful when done right because other checks may not reveal any potential problems in the applicant's background. Then because applicants tend to name people who they believe will give you favorable information about them, you should ask each reference to give you the name of someone else who has worked with the applicant. These secondary references will likely give you more objective information about the applicant. A good hiring policy would be to check three references named by the applicant and also three secondary references. Also, if you have anyone in your organization who has worked with the applicant, you should have an off-the-record conversation with them about the applicant.
- Test applicants for personality traits as well as job skills. Look for those who can work well with others, show compassion to and for others, respond well to criticism, and communicate frustrations effectively. Applicants that exhibit the following traits are worrisome:
  - An exaggerated view of their abilities, achievements, and potential value to an organization
  - Intolerant of criticism
  - Minimizes the significance of the work of others
  - Need for attention and approval
  - Excessively emotional
  - Overly moralistic
  - Strong beliefs on how things should be done
  - Unable to compromise, things are black or white and never gray, has the correct problem solution
  - Antisocial
  - Dishonest in background details and capabilities
  - Many job changes
  - Lawsuits with prior employers
  - Never had difficulties is past relationships
- Interview prospective employees. Seek to hire individual who are team-oriented, can respond well to criticism, and can deal well with conflicts, i.e., ones unlikely to become insider threats. Note that California employers are now prohibited from demanding usernames, passwords, and information related to social media accounts from job applicants and employees. The law also bans employers from firing or disciplining employees who refuse to divulge their social media information. This includes videos, photographs, blogs, podcasts, text messages, e-mail, online accounts, and website profiles. However, this prohibition does not apply to information used to access employer-issued electronic devices and is not intended to infringe on the existing rights and obligations of employers to investigate employee workplace misconduct or employee violations of other laws or regulations.
- Provide all employees with an employment manual that includes a strict code of conduct. Make sure all employees are aware of it. The code should include rules regarding times for lunch and breaks, purchases of store merchandise, use of supplies, etc.
- Inform employees about business security measures, e.g., surveillance and inventory checks, and the likelihood and consequences of being caught stealing. Many employees steal because they think they can easily get away with it.
- Keep a record of all employee purchases, exchanges, and refunds. Employees should not be permitted to ring up their own transactions.
- Provide lockers for employees. Require that employee's personal property and any store purchases be kept in their lockers during working hours.
- Prohibit employees from wearing or using store merchandise without purchasing it.
- Limit employee access to the building to the hours that they are scheduled to work.
- Have employees change jobs periodically. Do not announce changes in advance.
- Know your employees. Get views from people in various departments. Be alert to key indicators that an employee may become an insider threat. These include the following:
  - Sudden, apparent devotion to work and working late and alone
  - Accessing data not needed or never used in the past
  - Asking about things they are not involved with
  - Excessive use of "I" in writings and speech
  - Frustration with position and failure to get promoted
  - Lifestyle well above salary level
  - Financial debt
  - Strong objections to procedural changes related to financial, inventory or supply matters

    - Drugs and alcohol abuse
    - Moonlighting with materials available at the business
    - Evidence of compulsive gambling, persistent borrowing or bad check writing
- Make employees aware of insider threats and encourage employees to observe and collect information that indicates stress, and report suspicious behavior. The goal should be to catch an employee in the early stages of stress so they can be helped and prevented from harming themselves or the business.
- Develop protocols that will prevent a departing employee from stealing anything or later harming the business. Remind the employee of the agreements regarding confidentiality, non-disclosure of business information or data, and non-competition that were signed on employment.

CASH HANDLING

- Use serially, pre-numbered sales slips for every transaction. Encourage customers to expect a receipt by posting signs at each register.
- Conduct weekly audits. Have someone other than the sales clerk balance sales slips and register receipts.
- Make unannounced informal internal audits, and have a yearly audit performed by an outside firm.
- Put one employee in charge of setting up cash drawers. Have another double-check the cash count.
- Make each employee responsible for his/her cash drawer. Issue one cash drawer to each on-duty employee. No other employee should be allowed to open or use another's cash drawer at any time. At the end of each shift each cash drawer should be balanced by the employee and double-checked by another.
- Require that the cash register drawer be closed after each transaction. Never leave a register unlocked when not attended. And never leave the key with a register.
- Identify each over-ring and under-ring. Managers should sign off all voids and over-rings.
- Check signatures against those on file.
- Limit the amount of cash accumulated in any register. Use a drop-safe for excess cash.
- Check cash-to-sale ratios. These, along with unusually frequent refund transactions, can indicate employee theft.
- Keep tendered bills on the register until the transaction is concluded. Short-change artists frequently pay with large bills.
- Conduct only one transaction at a time. Do not be intimidated into rushing.
- Check for counterfeit currency. The look of the paper and its "feel" are usually the most obvious signs. A common counterfeiting practice is to "cut corners" off large bills and affix them to small-denomination bills. Inexpensive devices are available to aid detection of counterfeit bills.
- Make mail-opening and posting separate functions. Record checks and cash in appropriate registers, and stamp checks FOR DEPOSIT ONLY.

COMPUTER SECURITY

- Understand your computer systems and software. Have them designed so they cannot be used to divert money or inventory.
- Restrict access to computer terminals and records.
- Change entry codes periodically.
- Check regularly to ensure that security procedures are in effect.
- Include computer records in audits.
- For more information open the paper entitled *Cyber Security for Businesses* on the Prevention Tips page of the SDPD website at **www.sandiego.gov/police/services/prevention/tips**.

PROTECTION

- Shred all potentially sensitive materials including customer lists, price lists, medical prescription receipts, invoices, computer outputs, and documents with signatures.
- Require that all desks be cleared of important or confidential documents each night.
- Require that all file cabinets be locked when not in use.

INVENTORY CONTROL

- Separate receiving, storekeeping, and shipping functions.
- Conduct inventories often and at irregular intervals. Also make routine spot checks. Use new and more efficient inventory technologies, e.g., Radio Frequency Identification (RFID) tags that enable inventories to be done in hours instead of days.
- Inventories should be done annually by persons who are not responsible for inventory records.
- Inspect records of purchases and sales at the beginning and end of each shift.
- Define individual employee responsibilities for inventory control. This establishes a climate of accountability.
- Post signs to indicate areas that are open to the public and those that are for employees only. Install locks on all doors to interior work areas to control public and employee access. Doors to storage and supply rooms, and individual offices should be locked to limit access.
- Have all employees wear ID badges or some other means of distinguishing them from visitors, customers, and others on the premises. Businesses with restricted areas should give their employees photo-ID badges that are color-coded to indicate the areas that the employee is authorized to enter. Offices, storage and supply rooms, and other work areas should be checked periodically for the presence of unauthorized persons.
- Have all visitors in restricted areas be escorted by an employee who is authorized to be in those areas.

MAIL ROOM SECURITY

- Limit access to authorized, screened employees. Install access controls for employees, including cleaning and maintenance personnel.
- Give the Post Office a list of employees authorized to accept mail. Keep the list up to date as employees change over time.
- Make all work areas visible to supervisors. Use one-way glass, cameras, or elevated work stations for supervisors.
- Eliminate desk drawers and other places mail could be concealed.
- Have employees pick up their mail from a counter or desk that is separate from the area where incoming and outgoing mail is handled.
- Keep a log to establish accountability of registered and certified mail.
- Keep petty cash and postage stamps in a locked drawer.
- Restrict access to postage meters and keep it locked when not being used. Keep a record of meter register readings to detect possible unauthorized after-hours use.
- Prohibit employees from receiving personal mail.
- See U.S. Postal Service *Guide to Mail Center Security* at **http://about.usps.com/publications/pub166.pdf** for more a checklist and more actions to take.

TRASH CONTROL

- Keep trash dumpsters inside during business hours.
- Check bins at random times for pilfered goods that might have been placed in them for pick-up after the trash is taken out.
- Use clear plastic trash bags. Inspect bag contents for pilfered goods.
- Break down all cardboard boxes before putting them in dumpsters.
- Keep lids of outside trash dumpsters locked during non-business hours. If practical, keep the lids locked whenever the dumpsters are not being filled or emptied.
- Have employees work in pairs in emptying trash. Or have different employees empty the trash from day to day.

PURCHASING AND ACCOUNTING PROCEDURES

- Centralize purchasing but keep it separate it from receiving and accounting.
- Separate control of accounts payable and accounts receivable.
- Control purchase orders by pre-numbering them in sequence.

- Require supporting documentation for each purchase or expense invoice.
- Use pre-numbered checks in sequence. Type or print payees and amounts in permanent ink.
- Account for all checks in bank statements.
- Lock blank checks and a signature machine, if you have one, in a secure place.
- Don't allow the same employee to write checks and manage the books. Use two employees for these tasks or outsource the bookkeeping.
- Outsource some of your internal systems so red flags can be raised without the guilty employee's knowledge and ability to manipulate the system.
- Inform employees that there can be spot checks and audits at any time. Question expenditures that are unfamiliar or look out of line.
- Verify that new vendors in the books are legitimate.
- Have the mail room deliver bank statements to you before they are opened.

BANK DEPOSITS

Use an armored car service if possible. Otherwise assign two employees to make deposits. And vary the assignments over time.

KEY CONTROL

- Appoint a key control officer to manage the key and lock system.
- Keep keys in a locked cabinet or a secured area when they are not in use. Access can be by personal identification codes on keypads, card or fob readers, or biometric sensors. A key management system can restrict employee access to certain times, keep track of who has which keys, when keys should be returned, etc.
- Do not have a master key for all doors. Individual offices and restricted work areas should have separate keys.
- Issue as few keys as possible. Issue them only for areas the employee is authorized to be in. Keep up-to-date records of keys issued.
- Caution employees not to leave keys with parking lot attendants, in a topcoat hanging in a restaurant, or in their offices or work areas. This helps prevent keys from being taken and duplicated.
- Stamp keys DO NOT DUPLICATE.
- Code each key so that it does not need an identifying tag.
- Require departing employees to turn in all issued keys.
- Investigate all key losses.
- Re-key locks whenever a key is lost or when an employee leaves the business.
- Consider installing locks that are inexpensive to re-key. Or better to have a key-card system in which codes can be changed easily when a card is lost, entries and exits are recorded, etc.
- Seek advice from professional access control system designers.

ACCESS CONTROL CARDS

- Replace keys with access cards where practical. Cards are preferred because a record can be kept of their use, they cannot be duplicated and given to unauthorized persons, they can be deactivated when reported missing or when the employees authorization ends, their use can be limited to specific doors by time of day and day of week, and they can also be used to open parking lot or structure gates.
- Deactivate missing, lost, or stolen cards immediately on notice.
- At least annually, check that employees have their cards.
- Do not allow contractors and cleaners to keep cards. Have them sign out for and return them on a daily basis where practical.

SHIPPING AND RECEIVING PROCEDURES

- Establish receiving procedures that specify where vendors are allowed to park and enter the business.
- Do not permit trucks on the dock until they are ready to load or unload.

- Check all shipments against bills-of-lading. Number shipping orders in sequence to prevent padding or destruction.
- Recheck all incoming goods to prevent collusive thefts between the driver and the employees who handle the receiving.
- Do not permit drivers to load their own trucks or take goods from stock.
- Consider installing video cameras on the loading platforms. Locate the monitors where they can easily be seen by supervisors.

PROPERTY IDENTIFICATION

- Place the name of the business or some identification number on all business-owned items, e.g., office equipment, electronics, etc. This can be done by engraving or etching, using a permanent adhesive, or by attaching microdots. The owner's driver license number preceded by "CA" is suggested as a property identifier.
- Contractors can get information on preventing thefts of construction equipment and recovering stolen equipment by calling the Construction Industry Crime Prevention Program at **(562) 860-9006** or visiting its website at **www.crimepreventionprogram.com**. They can also obtain an Owner Applied Number (OAN) for large vehicles and heavy equipment. This number is usually stamped or engraved on your property and stored in a database in the National Crime Information Center (NCIC). Property with your OAN on it can be returned to you if it is recovered after being stolen. For an application, go to the website of the Agricultural Crime Technology Information and Operations Network (ACTION) at **www.agcrime.net**, click on REQUEST PUBLICATION, and download the brochure entitled *What is an OAN?* On the same website you can get additional information about OANs by clicking on TIPS TO PREVENT A CRIME, and then click on Owner Applied Number under PREVENT A CRIME ON YOUR PROPERTY.
- Keep a detailed, up-to-date record of your valuables. Include type, model, serial number, fair market value, etc. Photograph or videotape all valuables.

SELECTING CONTRACTORS

Businesses also have to be concerned with possible theft by contractor's employees. In selecting a contractor you should check its references and make sure it is insured and bonded. Insurance will protect you from damage caused by the contractor's employees. A surety bond will guarantee that the work will be performed as stated in the contract. For janitorial contractors you can require a janitorial services bond which will cover theft or other losses resulting from dishonest acts committed by an employee acting alone or in collusion with other persons. Some bonds require that the employee be prosecuted and convicted of the crime. Others require evidence of employee dishonesty. The conditions for coverage would be negotiated in drafting the bond.

You should also check that the contractor is licensed to work in the City of San Diego, i.e., that it has a Business Tax Certificate. This can be done on the Master Business Listing page of the City's website at **www.sandiego.gov/treasurer/taxesfees/btax/nblactive.shtml**. Construction contractors should be licensed by the State of California. You can check the status of a contractor's license on the Contractors State License Board's website at **www.cslb.ca.gov/default.asp**.

You can also require that the contractor conduct a background investigation on each employee that will work in your business. For this you will need to specify the following: (1) information an employee will have to provide, e.g., personal history, references, fingerprints, etc., (2) kinds of checks to be made, e.g., employee's name and SSN, criminal history, DMV record, credit record, civil action history, etc., and (3) criteria for passing each check, e.g., no criminal convictions or outstanding warrants, no bankruptcies, no civil judgments, etc. The contractor should also be prohibited from substituting a cleared employee with one that is not cleared, or subcontracting any of the services.

The opportunities for employee theft can be reduced by having the contract work done during normal business hours. This is the best option. Otherwise you'll have to give the contractor's employees means to enter the business when it is closed, or if the business is in an office building, both the building and its office suite, i.e., keys, door codes, or individual access cards, as well as the codes to any alarm systems that are installed. And the employee will have to lock all doors and turn on the alarm(s) when he or she leaves.

TECHNOLOGY SOLUTIONS

Employee theft involving gift cards is growing because the cards are like cash and it is a lot easier to leave a store with a card than an item of merchandise. Cashiers can fake refunds and then use their registers to fill in a gift card, which they take. Or when shoppers buy a card, they give them a blank card and divert the money into a card for themselves. However, the most common type of employee theft is "sweethearting," where cashiers fail to ring up or scan goods their friends or relatives bring to their register.

Technology solutions to these problems involve data mining programs and surveillance cameras. Data mining is used to determine whether one cashier is refunding far more items than other cashiers. And cameras can show whether a cashier repeatedly gave refunds to the same friend or relative, or whether a cashier failed to run merchandise over the scanner.